Cisco SNMP Installation and Basic Configuration

Installation Prerequisites for SNMP Support

Unified CCE SNMP support is automatically installed during the course of normal setup. No extra steps need be taken *during* setup for SNMP support to be enabled. However, Microsoft Windows SNMP optional components must be installed on Unified ICM/CCE servers for any SNMP agents to function.

Install the appropriate Microsoft Windows SNMP component(s) before installing any Unified ICM CCE components that require SNMP monitoring. Following are the instructions to install the Microsoft Windows SNMP components.

Note The Microsoft SNMP component(s) are required for Cisco SNMP support. The Microsoft Windows SNMP service is disabled as part of web setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place. The Cisco Contact Center SNMP Management service provides for more sophisticated SNMP capabilities than the standard Microsoft SNMP Service.

Install Microsoft Windows SNMP Components on Windows Server

See the Microsoft documentation to install Microsoft Windows SNMP components on the Windows Server.

Cisco Contact Center SNMP Solution Configuration

The Cisco Contact Center SNMP solution is configurable from a Microsoft Management Console (MMC) Snap-in.

Basic Configuration

While all SNMP components are installed and enabled by default, the device is not manageable via an NMS until the solution is properly configured. For security reasons, certain parameters are not configured by default.

The system administrator must configure the following to grant access to the agents and enable the receipt of SNMP notifications:

1. Configure the Community Name or User Names:
   - If you are using SNMP version 1 or version 2c, at least one community string must be configured on each Unified ICM/CCE server to be managed (see below), OR
   - If using SNMP version 3, configure at least one user name on each Unified ICM/CCE server to be managed (see below).
2. Configure General Properties.
3. For trap forwarding, configure an SNMP trap destination on each Unified ICM/CCE Logger server. You can also optionally add a Syslog Destination.

You can use the Cisco SNMP Agent Management MMC Snap-in to configure all properties.

Note Some diagnostic tools use SNMP locally to gather information about the system using one of the community strings configured for Windows SNMP. These community strings are not added to the Contact Center SNMP configuration, which causes SNMP requests from these diagnostic tools to fail. Add all communities configured for Windows SNMP to the Contact Center SNMP configuration. It is not necessary for the Windows SNMP service to be started or enabled. To find the Windows SNMP communities in the "Security" tab select "properties" for the Windows SNMP service from the list of Windows services.

Related Topics

General Properties Configuration, on page 5
Configuration of Trap and Syslog Destinations, on page 6

Add Cisco SNMP Agent Management Snap-In

You can configure Cisco SNMP Agent Management settings using a Windows Management Console Snap-in. To add the Snap-in and change Cisco SNMP Management settings:

Procedure

Step 1 From the Start menu select **Run.**.

Step 2 In the Start box type in `mmc/32` and press ENTER.

Attention The Cisco SNMP Agent Management Snap-In is a 32-bit snap-in and is only available when the "/32" switch is used.

Step 3 From the Console, select **File** > **Add/Remove Snap-in**

A new window appears.

Step 4 From the **Selected Snap-ins** tab, verify **Console Root** is selected in the **Snap-ins added to:** field and click **Add.**

Step 5 In the **Available Snap-ins** window, scroll down and select **Cisco SNMP Agent Management**.

Step 6 In the **Add Snap-in** window click **Add**.

Step 7 In the **Add Snap-in** window click **Close**.

Step 8 Click **OK** in the **Add/Remove Snap-in** window.
The Cisco SNMP Agent Management Snap-in is now loaded in the console.

Saving Snap-In View

After you load the Cisco SNMP Agent Management MMC Snap-in, you can save that console view to a file (with a .MSC file extension) that you can launch directly, instead of repeatedly adding the Snap-in to a new MMC console view. To do so, select the **File** > **Save As** menu; a **Save As** dialog appears.

Select a memorable file name such as **Cisco SNMP Agent Management.msc** (retain the .msc file extension) and save the file to the desired location. The Administrative Tools (start) menu is the default location, which makes it conveniently available for later access via the Start menu.

Configure Community Name for SNMP v1 and v2c

If you use SNMP v1 or v2c, configure a Community Name so that the Network Management Stations (NMSs) can access the data that your server provides. These names are left blank during the installation for security reasons.

SNMP Community Names are used to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same Community Name.

To configure the Community Name for SNMP v1 and v2c:

Procedure

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Community Names (SNMP v1/v2c)** in the left pane under Cisco SNMP Agent Management. Community Name, SNMP Version, and Restricted Access columns appear in the middle pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.
A dialog box appears.

Step 5 Click **Add new Community**.

Step 6 In the dialog box, under **Community Information**, provide a community name.

Step 7 Select the **SNMP Version** by selecting the radio box for SNMP V1 or SNMP V2c.

Step 8 Optionally, enter one or more IP addresses in the IP Address entry field (containing “dots”). Click **Insert** to enable the access solely for this community from the NMS with the IP Address provided.

Step 9 Click **Save**.

The community name appears in the **Configured Communities** section at the top of the dialog box.

Note You can remove the community name by highlighting the name in the **Configured Communities** section and clicking **Remove Community**.

Changes become effective when you click **OK**.

Configure User Name for SNMP v3

If you are using SNMP v3 you must configure a User Name so that Network Management Stations (NMSs) can access the data provided by your server. By default, these names are left blank for security reasons.

To configure a User Name for SNMP v3:

Procedure

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **User Names (SNMP v3)** in the left pane under Cisco SNMP Agent Management.
User Name, Authentication, Privacy, and Restricted Access columns appear in the middle pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.
A dialog box appears.

Step 5 Click **Add User**.

Step 6 In the **User Configuration** text box enter a user name.

Step 7 If you wish to use SNMP v3 authentication, check **Required?** under Authentication, choose an authentication protocol, then enter and confirm a password.

This setting encrypts the password information as it is sent over the network.

Note These settings must also be used on your NMS to access SNMP data from this server.

Step 8 If you wish to use SNMP v3 privacy, check **Required?** under Privacy, choose an encryption type, and enter and confirm a password.

Note
- This setting encrypts all SNMP information as it is sent over the network. If privacy is configured, authentication is required, but authentication can be configured without configuring privacy.
- These settings must also be used on your NMS to access SNMP data from this server.

Step 9 Optionally, enter one or more IP addresses in the IP Address entry field (containing “dots”) and click **Insert** to enable access solely from the NMS with the IP Address provided.

Step 10 Click **Save**.

The User Name appears in the **Configured Users** section at the top of the dialog box.

Note You can remove the User Name by highlighting the name in the **Configured Users** section and clicking **Remove User**.

Changes become effective when you click **OK**.

Related Topics

Configuration of Trap and Syslog Destinations, on page 6

General Properties Configuration

Use the Cisco Contact Center SNMP Solution Configuration to access the configuration screens.

Configure General Information Properties for Cisco SNMP Agent Management

You can configure general information properties for Cisco SNMP within the Cisco SNMP Agent Management Snap-in.

To configure general information properties:

Procedure

Step 1 In the Cisco SNMP Agent Management Snap-in, expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 2 Highlight **General Information** in the left pane under Cisco SNMP Agent Management.
Attribute, Value, and Description columns appear in the middle pane.

Step 3 Right click on the white space in the middle pane and choose **Properties**.
A dialog box appears.

Step 4 You can change the following properties in the **SNMP System Information** section of the General Information Properties dialog box.

Table 1: SNMP System Information Properties

Property	Description
System name	The fully qualified domain name of the system. If system name is empty, it is automatically filled in.
System Location	A text area to describe the location of the hardware. For example `Building 5, Floor 3, Room 310.`
System Contact	The name, email address and/or telephone number of the system contact. Enter anything that aids an NMS user in contacting the system administrator.
System Description	A brief description of this system.
SNMP Port Number	The default port for SNMP applications is UDP 161. If your NMS uses a different port, you can change that value here.
Enable Authentication Traps	Check if you wish to enable Authentication Traps. When a device receives an authentication that fails, the device sends a trap to the NMS.

Step 5 You can change the Windows Execution Priority of the Cisco SNMP agents in the **Agent Performance** section under **Execution Priority**. The default is *Below Normal.* You can further lower it by setting it to *Low.* Keep the settings at the default levels unless you see a significant performance impact.

Step 6 You can also further modify SNMP Agent Performance by changing the number of *Concurrent Requests, Subagent Wait Time* (in seconds), and *Subagents.* the default values are 5, 25, and 25 respectively. Keep the settings at the default levels unless you see a significant performance impact.

Definitions:

Concurrent requests
The maximum number of SNMP requests that a subagent can concurrently process. Any pending requests above this value are queued.
Subagent Wait Time
The maximum number of seconds that the master agent waits for a subagent response.
Subagents
The maximum allowable subagents that the master agent loads.

Step 7 To change the amount of information written to the SNMP logs, choose Verbose (most information), Normal (Default), or Terse (least information). Only change this value under direction from Cisco Technical Assistance (TAC).

Step 8 Click **OK** to save changes that you made.

Configuration of Trap and Syslog Destinations

Use the Cisco Contact Center SNMP Solution Configuration to access the configuration screens.

Note Restarting the service does not clear conflicts between host address and SNMP destination. When there is a conflict between the host address list and the SNMP Trap Destination, if you delete the items from the host address list, and restart the service, the configuration is reset.

Configure SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c and SNMP v3. A Trap is a notification used by the SNMP agent to inform the NMS of a certain event.

Follow these steps to configure the trap destinations:

Procedure

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Trap Destinations** in the left pane under Cisco SNMP Agent Management.
Trap Entity Name and SNMP Version columns appear in the right pane.

Step 4 Right click on the white space in the middle pane and choose **Properties**.

A dialog box appears.

Step 5 Click **Add Trap Entity**.

Step 6 Under **Trap Entity Information** select the SNMP version radio box for the version of SNMP used by your NMS.

Step 7 Provide a name for the trap entity in the **Trap Entity Name** field.

Step 8 Select the SNMP Version Number.

Step 9 Select the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing users/community names that have already been configured.

Step 10 Enter one or more IP addresses in the IP Address entry field (containing "dots") and click **Insert** to define the destination(s) for the trap(s).

Step 11 Click **Save** to save the new trap destination.

The Trap Entity Name appears in the **Trap Entities** section at the top of the dialog box.

Note You can remove the Trap Entity by highlighting the name in the **Trap Entities** section and clicking **Remove Trap Entity**.

Step 12 Changes become effective when you click **OK**

Configure Syslog Destinations

You can configure Syslog destinations for SNMP from the Cisco SNMP Agent Management Snap-in. The syslog feed is only available on the Unified ICM/CCE Logger Node.

Before you configure the syslog destinations, you must start the syslog process (cw2kfeed.exe) from the Web Setup tool.

1. Open the Web Setup tool
2. Select **Component Management > Loggers,** and then choose the instance of the logger for which you want to enable the syslog event feed.
3. In the Additonal Options area, check the **Enable Syslog** check box to enable the syslog event feed process.

These steps runs the CW2KFEED process when the logger is started.

Follow these steps to configure Syslog destinations:

Procedure

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Syslog Destinations** in the left pane under Cisco SNMP Agent Management.
ICM Instance Name, Feed Enabled, Collector Address, Port, and Ping Disabled columns appear in the right pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.
A dialog box appears.

Step 5 Select an Unified ICM/CCE Instance from the list box.

Step 6 Check the **Enable Feed?** checkbox.

Step 7 In the **Collector Address** field, enter the IP address or Host Name.

Step 8 (Optional) In the **Collector Port** field, enter the collector port number on which syslog collector is listening.

Note The default port is 514.

Step 9 (Optional) Check the **Disable Ping Tests?** checkbox.

Step 10 Click **Save**.

Step 11 Changes become effective when you click **OK** and restart the logger.

Manage SNMP Service

In general, the Cisco Contact Center SNMP Management Service is always running.

To confirm that the Cisco Contact Center SNMP Management Service is running or to restart or stop it, follow these steps:

Procedure

Step 1 From the Windows desktop, choose **Start** > **Settings** > **Control Panel**.

Step 2 Double-click **Administrative Tools**.

Step 3 Double-click **Services**.

The **Services** window appears.

Step 4 Look at the Status field in the **Cisco Contact Center SNMP Management service** row.

If this field displays “Started,” the Cisco Contact Center SNMP Management Service is running. If this field is blank, the Cisco Contact Center SNMP Management Service is not running.

To start the Cisco Contact Center SNMP Management Service, right-click **Cisco Contact Center SNMP Management** and choose **Start**.

To stop the Cisco Contact Center SNMP Management Service, right-click SNMP Service and choose **Stop**.

To restart the Cisco Contact Center SNMP Management Service, right-click **Cisco Contact Center SNMP Management** and choose **Restart**.